COMPOSITIO MATHEMATICA

Zeros of systems of $\mathfrak{p}$-adic quadratic forms

D. R. Heath-Brown

Compositio Math. **146** (2010), 271–287.

doi:10.1112/S0010437X09004497

FOUNDATION COMPOSITIO MATHEMATICA

The London Mathematical Society

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

Compositio Math. 146 (2010) 271–287
doi:10.1112/S0010437X09004497

Zeros of systems of $\mathfrak{p}$-adic quadratic forms

D. R. Heath-Brown

Abstract

We show that a system of r quadratic forms over a $\mathfrak{p}$-adic field in at least $4r+1$ variables will have a non-trivial zero as soon as the cardinality of the residue field is large enough. In contrast, the Ax–Kochen theorem [J. Ax and S. Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630] requires the characteristic to be large in terms of the degree of the field over $\mathbb{Q}_p$. The proofs use a $\mathfrak{p}$-adic minimization technique, together with counting arguments over the residue class field, based on considerations from algebraic geometry.

1. Introduction

Let K be a finite extension of $\mathbb{Q}_p$ with associated prime ideal $\mathfrak{p}$, and let $q^{(i)}[x_1, \ldots, x_n] \in K[x_1, \ldots, x_n]$ be quadratic forms, for $1 \leqslant i \leqslant r$. It would follow from the conjecture of Artin [Art65, Preface] that these forms have a simultaneous non-trivial zero in K^n, providing only that $n > 4r$. Although Artin's conjecture is known to be false in general (see [Ter66], for example), this particular consequence of the conjecture is still an open problem. The two cases $r = 1$ and $r = 2$ have been successfully handled, the former by Hasse [Has24] and the latter by Demyanov [Dem56]. For $r = 3$ it has been shown by Schuur [Sch80] that $n \geqslant 13$ suffices when the residue field has odd characteristic and cardinality at least 11. No analogous result for $r \geqslant 4$ has been established until now. However, it follows from the work of Ax and Kochen [AK65] that if the degree $[K : \mathbb{Q}_p] = D$ is given, then $n \geqslant 4r + 1$ variables suffice as soon as $p \geqslant p(r, D)$, for some prime $p(r, D)$. The proof uses methods from mathematical logic, and does not yield a practical value for $p(r, D)$.

If one is willing to allow more variables, then further results are available. Thus Leep [Lee84] has shown that it suffices to have $n \geqslant 2r^2 + 2r - 3$ as soon as $r \geqslant 2$, for any $\mathfrak{p}$-adic field K, and Martin [Mar97] has improved this further to allow $n \geqslant 2r^2 + 3$ if r is odd and $n \geqslant 2r^2 + 1$ if r is even. One can do a little better for large r, but the bound on n is asymptotically $2r^2$ in all such results.

The purpose of the present paper is to develop an analytic method which will establish the following result.

Theorem. *Let K have residue field F and suppose that $\#F = q$. Then the quadratic forms $q^{(1)}, \ldots, q^{(r)}$ have a non-trivial common zero over K as soon as $n \geqslant 4r + 1$, providing that $q \geqslant (2r)^r$. More specifically, it suffices that $q > n \geqslant 4r + 1$ and $\sigma_1 + \sigma_2 < 1$, where*

$$\sigma_1 = q^{r-n} + \sum_{\lceil n/2r \rceil - 1 \leqslant t \leqslant n/2} q^{-t} \left(\frac{q}{2t+1} \right)^{[4rt/n]} (2t+1)^r$$

Received 13 October 2008, accepted in final form 29 July 2009, published online 22 January 2010.
2000 Mathematics Subject Classification 11E08 (primary), 11D72, 11D79, 11D88 (secondary).
Keywords: quadratic form, system, $\mathfrak{p}$-adic field, zeros, Ax–Kochen theorem.

and

$$\sigma_2 = \frac{1}{q-1}\sum_{\rho=2(\lceil n/2r\rceil-1)}^{n-1}\ \sum_{0\leqslant t\leqslant(n-\rho)/2} C_{\rho,t}q^{-\rho-t+[2r\rho/n]+[2r(\rho+2t)/n]}$$

with

$$C_{\rho,t} = (\rho+1)^{r-[2r\rho/n]}(2t+1)^{r-[2r(\rho+2t)/n]}.$$

Here we use the notation

$$\lceil\theta\rceil = \min\{n\in\mathbb{Z} : n\geqslant\theta\}.$$

Some small improvements in the values of σ_1 and σ_2 are possible, but these have little effect on the range of q that one can handle.

It should be emphasized that the Ax–Kochen theorem gives no information about fields with a fixed characteristic p. Thus it leaves open the possibility that Artin's conjecture is *never* true for dyadic fields, for example. In contrast, our result shows that it is sufficient to have $\#F$ large enough.

We have the following corollary. The $r=8$ case will be of relevance later.

Corollary 1. *It suffices to have $n\geqslant 4r+1$ in the following cases:*

(i) $r=3$ *and* $q\geqslant 37$;
(ii) $r=4$ *and* $q\geqslant 191$;
(iii) $r=8$ *and* $q\geqslant 271\,919$.

As an indication of what can be achieved for larger values of n we investigate the condition $n>r^2$, which may be compared with Martin's result [Mar97] mentioned above, where one requires that $n\geqslant 2r^2+3$ if r is odd and $n\geqslant 2r^2+1$ if r is even, for any q.

Corollary 2. *It suffices to have $n\geqslant r^2+1$, providing that $r\geqslant 5$ and $q\geqslant(4\times 10^8)r^2$.*

The coefficient in front of r^2 can certainly be improved, but the importance of the result is that we require a lower bound for q which is only a power of r. However, we have been unable to eliminate entirely the need for a lower bound on q, even for n as large as $2r^2$.

The $r=8$ case is of relevance to the problem of p-adic zeros of quartic forms. The author has shown in [Hea09] that if $p\neq 2,5$, then any quartic form over $\mathbb{Q}_p$ in n variables has a non-trivial p-adic zero, providing that any system of 16 linear forms and 8 quadratic forms also has a non-trivial zero. Our results therefore have the following corollary.

Corollary 3. *A quartic form over $\mathbb{Q}_p$ in at least 49 variables has a non-trivial p-adic zero providing that $p\geqslant 271\,919$.*

Our proofs use a $\mathfrak{p}$-adic minimization technique, for which see Birch and Lewis [BL65, Lemma 12]. Let F be the residue field. Then, as in [BL65, §§ 3–4], it suffices to prove our theorem for 'minimized' systems of forms $q^{(i)}$. Such forms will have $\mathfrak{p}$-adic integer coefficients, and we write $Q^{(i)}(x_1,\ldots,x_n)\in F[x_1,\ldots,x_n]$ for their reductions in F. In view of Hensel's lemma, it will suffice to find a non-singular zero in F^n for the system $Q^{(i)}=0$. The minimization process ensures that the forms $Q^{(i)}$ will satisfy a key condition, given by [BL65, Lemma 12(2)]. We proceed to explain this condition.

Suppose $S^{(1)},\ldots,S^{(s)}$ are linearly independent forms taken from the F-pencil generated by the $Q^{(i)}$. Suppose further that after a linear change of variables, the forms

$$S^{(i)}(0,\ldots,0,x_{w+1},\ldots,x_n),\quad 1\leqslant i\leqslant s$$

all vanish identically. Then if the original system $q^{(i)}$ was minimized, [BL65, Lemma 12(2)] tells us that

$$w \geqslant \frac{sn}{2r}. \tag{1}$$

In particular, if $n > 4r$, we must have $w > 2s$. As an example of the minimization condition (1), take $n > 4r$ and $s = 1$, whence we deduce that $w \geqslant 3$. Thus no form S in the pencil can be annihilated by setting two variables equal to zero. In particular, if there were any form S in the F-pencil which had rank at most two, we could express it as a function of x_1 and x_2 only, allowing $w = 2$ and thereby obtaining a contradiction. Indeed, if there were a form of rank three, it could be written as $S(x_1, x_2, x_3)$ and by Chevalley's theorem we could take $S(0, 0, 1) = 0$, which again permits $w = 2$. We therefore conclude that if $n > 4r$, the condition (1) implies that every non-zero form in the F-pencil has rank at least four.

We can now focus on systems $Q^{(i)}$ over the finite field F. As noted above, it suffices to find a non-singular zero, given the key minimization condition (1). This will be done by a counting argument, in which we first give a lower bound estimate for the total number of solutions to the system $Q^{(i)} = 0$, and then give an upper bound on the number of singular solutions. Here a major rôle will be played by singular forms in the F-pencil generated by the $Q^{(i)}$. We will therefore be forced to consider how many forms of a given rank the pencil can contain, and this problem is the key point in the proof. Our treatment will use some algebraic geometry ultimately motivated by the work of Davenport [Dav63, § 2], and it is at this point that the minimization condition (1) is applied.

2. Geometric considerations

In discussing the geometry of our system of quadratic forms, we shall work over the algebraic closure $\overline{F}$. Thus, when we speak of a point on a variety V, we shall mean an $\overline{F}$-point, unless we explicitly write $V(F)$. We shall take special care to include the case in which F is dyadic. We write $\chi(F)$ for the characteristic of F. Although F will be a finite field in our application, for the generalities discussed below it suffices for F to be a perfect field. However, the situation can be different when F is not perfect. To begin with, we will not assume that condition (1) holds.

We start by attaching a symmetric $n \times n$ matrix $M^{(i)}$ to each form $Q^{(i)}$. In general, if

$$Q(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} a_{ij} x_i x_j,$$

then the associated matrix will have entries

$$M_{ij} = \begin{cases} a_{ij} & \text{for } i < j, \\ 2a_{ii} & \text{for } i = j, \\ a_{ji} & \text{for } i > j. \end{cases} \tag{2}$$

When $\chi(F) \neq 2$, this corresponds to the usual definition. For $\chi(F) = 2$, the matrix M is skew-symmetric and always has even rank.

By the rank of a quadratic form Q we mean the minimal r such that there is a form Q' over F, in r variables, and linear forms

$$L_1(x_1, \ldots, x_n), \ldots, L_r(x_1, \ldots, x_n)$$

over F for which

$$Q(x_1, \ldots, x_n) = Q'(L_1, \ldots, L_r).$$

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

It is not hard to show that the rank of a form is independent of the field over which one works. When $\chi(F) \neq 2$ one has $\mathrm{Rank}(Q) = \mathrm{Rank}(M)$, but this is not true in general if $\chi(F) = 2$. However, we always have

$$\mathrm{Rank}(M) = 2[\mathrm{Rank}(Q)/2]$$

for dyadic fields.

When $\chi(F) \neq 2$, the condition $\mathrm{Rank}(Q) \leqslant R$ is equivalent to the vanishing of all the $(R+1) \times (R+1)$ minors of M. When $\chi(F) = 2$ and R is odd, we have $\mathrm{Rank}(Q) \leqslant R$ if and only if $\mathrm{Rank}(M) \leqslant R - 1$. Hence in this case a necessary and sufficient condition is that the $R \times R$ minors of M all vanish. When $\chi(F) = 2$ and R is even, the picture is slightly more complicated. A necessary and sufficient condition for the rank of Q to be at most R is that $\mathrm{Rank}(M) \leqslant R$ and that if $\mathrm{Rank}(M) = R$, then Q vanishes on a set of generators for the null space of M. However, if $\mathrm{Rank}(M) = R$ the null space is generated by vectors $\mathbf{v}_1, \ldots, \mathbf{v}_{n-R}$ whose components are $R \times R$ minors of M, while if $\mathrm{Rank}(M) < R$ these vectors will vanish. It follows that if $\chi(F) = 2$ and R is even, then $\mathrm{Rank}(Q) \leqslant R$ if and only if $\mathrm{Rank}(M) \leqslant R$ and $Q(\mathbf{v}_i) = 0$ for $i \leqslant n - R$. Thus in each case there is a set of polynomial conditions on the coefficients of Q which determines whether or not $\mathrm{Rank}(Q) \leqslant R$. If we now define

$$V_R = \left\{ [\mathbf{u}] \in \mathbb{P}^{r-1} : \mathrm{Rank}\left\{ \sum_{i=1}^{r} u_i Q^{(i)} \right\} \leqslant R \right\}, \tag{3}$$

it follows that V_R is an algebraic set. We have shown that these polynomial conditions defining V_R are of degree at most $R+1$ in $\mathbf{u}$ unless $\chi(F) = 2$ and R is even, in which case they have degree $2R+1$. In the final section of this paper we will establish the following improvement.

Lemma 1. *When F is a perfect field with $\chi(F) = 2$ and R is even, there is a set of forms of degree $R+1$ in the coefficients of the quadratic form Q which vanish if and only if* $\mathrm{Rank}(Q) \leqslant R$.

Suppose that we have a point $[\mathbf{u}_0]$ which lies in $V_R(F)$ but not in V_{R-1}, where we conventionally take $V_{-1} = \emptyset$. Then $[\mathbf{u}_0]$ will belong to some component W, say, of V_R. We proceed to bound the dimension of W.

Let $k = n - R$ and let G be the Grassmannian of $(k-1)$-dimensional linear spaces $L \subseteq \mathbb{P}^{n-1}$. Then $\mathrm{Rank}(Q) \leqslant R$ if and only if there is an $L \in G$ such that $M\mathbf{x} = \mathbf{0}$ and $Q(\mathbf{x}) = 0$ for all $[\mathbf{x}] \in L$. We use the notation $ML = 0$ and $Q(L) = 0$ for these latter conditions. If $\mathrm{Rank}(Q) = R$, the space L will be unique and will be defined over F. If N is the vector space corresponding to L, so that $\dim(N) = k$, we say that N is the null space for Q.

Let

$$J = \left\{ ([\mathbf{u}], L) \in W \times G : \left(\sum_{1}^{r} u_i M^{(i)} \right) L = 0, \left(\sum_{1}^{r} u_i Q^{(i)} \right)(L) = 0 \right\}.$$

When we project from J to W the fibre above any point is non-empty, whence $\dim(J) \geqslant \dim(W)$.

It is now convenient to change the basis for the F-pencil generated by the forms $Q^{(i)}$ so that $\mathbf{u}_0$ becomes $(1, 0, \ldots, 0)$. We then put $Q = Q^{(1)}$, so that Q has rank exactly R. Let N be the null space for Q, and make a linear change of variables so that N is generated by the first k unit vectors $\mathbf{e}_1, \ldots, \mathbf{e}_k$. We would like to examine the tangent space of J at $([\mathbf{u}_0], L_0)$, where L_0 is the projective linear space corresponding to N. This tangent space is most readily identified by switching to the affine setting. We therefore define

$$V = \{\mathbf{v} = (v_2, \ldots, v_r) \in \mathbb{A}^{r-1} : [(1, \mathbf{v})] \in W\}$$

and

$$Y = \{\mathbf{y} \in \mathbb{A}^n : y_1 = \cdots = y_k = 0\}.$$

Notice that $\mathbf{0} \in V$ and that $\dim(V) = \dim(W)$.

We now consider the algebraic set $Z \subseteq V \times Y^k$ specified by the condition $v \in V$ along with the equations

$$\left\{M + \sum_{i=2}^{r} v_i M^{(i)}\right\}(\mathbf{e}_j + \mathbf{y}_j) = \mathbf{0}, \quad 1 \leqslant j \leqslant k$$

and

$$\left\{Q + \sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{e}_j + \mathbf{y}_j) = 0, \quad 1 \leqslant j \leqslant k.$$

Thus we have $nk + k$ equations, in addition to the condition $v \in V$. Note that our equations imply that $\{Q + \sum_i v_i Q^{(i)}\}(\mathbf{w}) = 0$ for any $\mathbf{w}$ in the span of the vectors $\mathbf{e}_j + \mathbf{y}_j$. Thus Z is an affine version of J, with the linear space L corresponding to the vector space generated by $\mathbf{e}_j + \mathbf{y}_j$ for $1 \leqslant j \leqslant k$. In particular, it follows that

$$\dim(Z) = \dim(J) \geqslant \dim(W).$$

One can now calculate the tangent space $\mathbb{T} = \mathbb{T}(Z, (\mathbf{0}, \ldots, \mathbf{0}))$. One finds that $\mathbb{T}$ is the set of $(\mathbf{v}, \mathbf{y}_1, \ldots, \mathbf{y}_k) \in \mathbb{T}(V, \mathbf{0}) \times Y^k$ which satisfy the equations

$$\left\{\sum_{i=2}^{r} v_i M^{(i)}\right\}\mathbf{e}_j + M\mathbf{y}_j = \mathbf{0}, \quad 1 \leqslant j \leqslant k \tag{4}$$

and

$$\left\{\sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{e}_j) + \mathbf{y}_j^T \nabla Q(\mathbf{e}_j) = 0, \quad 1 \leqslant j \leqslant k.$$

However, we have $\nabla Q(\mathbf{e}_j) = M\mathbf{e}_j = \mathbf{0}$, so the second set of conditions reduces to

$$\left\{\sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{e}_j) = 0, \quad 1 \leqslant j \leqslant k. \tag{5}$$

If $(\mathbf{v}, \mathbf{y}_1, \ldots, \mathbf{y}_k) \in \mathbb{T}$, we may pre-multiply the relation (4) by $\mathbf{e}_h^T$ for any $h \leqslant k$ and use the fact that $\mathbf{e}_h^T M = \mathbf{0}^T$ to deduce that

$$\mathbf{e}_h^T \left\{\sum_{i=2}^{r} v_i M^{(i)}\right\}\mathbf{e}_j = 0, \quad 1 \leqslant j, h \leqslant k. \tag{6}$$

The two conditions (5) and (6) now imply that

$$\left\{\sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{x}) = 0 \quad \text{for all } \mathbf{x} \in N. \tag{7}$$

Let $\pi : \mathbb{T} \to \mathbb{T}(V, \mathbf{0})$ be the natural projection. Then the relation (7) holds for any $\mathbf{v} \in \pi(\mathbb{T})$. However, π is a linear map between vector spaces, and

$$\mathrm{Ker}(\pi) = \{(\mathbf{0}, \mathbf{y}_1, \ldots, \mathbf{y}_k) \in \{\mathbf{0}\} \times Y^k : \ M\mathbf{y}_j = \mathbf{0} \text{ for } 1 \leqslant j \leqslant k\}.$$

When $\chi(F) \neq 2$, the matrix M has null space N; so we must have $\mathbf{y}_j = \mathbf{0}$ for all j, whence $\mathrm{Ker}(\pi)$ is trivial. When $\chi(F) = 2$, the matrix M will have null space N only when R is even;

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

thus, in the dyadic case we now require R to be even. Under this assumption we will have $\dim(\pi(\mathbb{T})) = \dim(\mathbb{T})$, whence

$$\dim(\pi(\mathbb{T})) = \dim(\mathbb{T}) \geqslant \dim(Z) = \dim(J) \geqslant \dim(W),$$

since the tangent space of Z at any point has dimension at least as large as Z itself.

Since $Q^{(1)}(\mathbf{x}) = Q(\mathbf{x}) = 0$ for all $\mathbf{x} \in N$, we now deduce that there is a vector space, with dimension at least $1 + \dim(W)$, of quadratic forms in the $\overline{F}$-pencil that all vanish on the space N. However, N is defined over F itself, and hence

$$\left\{\mathbf{u} \in \mathbb{A}^r : \left\{\sum_1^r u_i Q^{(i)}\right\}(\mathbf{x}) = 0 \text{ for all } \mathbf{x} \in N\right\}$$

is also defined over F. We therefore draw the following conclusion.

Lemma 2. *Let V_R be the variety (3). Suppose either that $\chi(F) \neq 2$, or that $\chi(F) = 2$ and R is even. Suppose further that we have a point $\mathbf{u} \in F^r$ for which the form*

$$Q = \sum_{i=1}^r u_i Q^{(i)} \tag{8}$$

has rank R and null space N and such that $[\mathbf{u}]$ belongs to an irreducible component W of V_R. Then there are at least $1 + \dim(W)$ linearly independent quadratic forms $S^{(i)}$ in the F-pencil (8), all of which vanish on the F-vector space N of codimension R in F^n.

To handle the case in which $\chi(F) = 2$ and R is odd, we need to make a small modification of the previous argument. We keep the same notation as before, but in addition to the null space N of Q we must now consider the null space N_0 of M. In the previous situation these null spaces coincided, but now N is strictly contained in N_0. If we write G_0 for the Grassmannian of k-dimensional linear subspaces of $\mathbb{P}^{n-1}$, then N and N_0 will correspond to some pair of linear spaces $L \in G$ and $L_0 \in G_0$, with $L \subset L_0$. We now define

$$J_0 = \left\{([\mathbf{u}], L, L_0) \in W \times G \times G_0 :\ L \subset L_0,\ \left(\sum_1^r u_i M^{(i)}\right) L_0 = 0,\ \left(\sum_1^r u_i Q^{(i)}\right)(L) = 0\right\}.$$

As before, when we project from J_0 to W, the fibre above any point is non-empty, whence $\dim(J_0) \geqslant \dim(W)$.

Following the previous analysis, we switch to affine coordinates. We change variables as before, so that $Q = Q^{(1)}$ and so that N and N_0 are generated by $\mathbf{e}_1, \ldots, \mathbf{e}_k$ and $\mathbf{e}_1, \ldots, \mathbf{e}_{k+1}$, respectively. We use the same set V as before but now take

$$Y = \{\mathbf{y} \in \mathbb{A}^n : y_1 = \cdots = y_{k+1} = 0\}.$$

This time we define a set $Z_0 \subseteq V \times Y^{k+1}$ specified by the condition $v \in V$ along with the equations

$$\left\{M + \sum_{i=2}^r v_i M^{(i)}\right\}(\mathbf{e}_j + \mathbf{y}_j) = \mathbf{0}, \quad 1 \leqslant j \leqslant k+1$$

and

$$\left\{Q + \sum_{i=2}^r v_i Q^{(i)}\right\}(\mathbf{e}_j + \mathbf{y}_j) = 0, \quad 1 \leqslant j \leqslant k.$$

Again, we note that Z_0 is an affine version of J_0, whence $\dim(Z_0) = \dim(J_0) \geqslant \dim(W)$.

The tangent space $\mathbb{T}_0 = \mathbb{T}(Z_0, (\mathbf{0}, \ldots, \mathbf{0}))$ is the set of $(\mathbf{v}, \mathbf{y}_1, \ldots, \mathbf{y}_{k+1}) \in \mathbb{T}(V, \mathbf{0}) \times Y^{k+1}$ which satisfy the equations

$$\left\{\sum_{i=2}^{r} v_i M^{(i)}\right\}\mathbf{e}_j + M\mathbf{y}_j = \mathbf{0}, \quad 1 \leqslant j \leqslant k+1$$

and

$$\left\{\sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{e}_j) = 0, \quad 1 \leqslant j \leqslant k.$$

As before, these imply that

$$\left\{\sum_{i=2}^{r} v_i Q^{(i)}\right\}(\mathbf{x}) = 0 \quad \text{for all } \mathbf{x} \in N.$$

If $\pi_0 : \mathbb{T}_0 \to \mathbb{T}(V, \mathbf{0})$ is the natural projection, then the above relation holds for any $\mathbf{v} \in \pi(\mathbb{T}_0)$. However,

$$\mathrm{Ker}(\pi_0) = \{(\mathbf{0}, \mathbf{y}_1, \ldots, \mathbf{y}_{k+1}) \in \{\mathbf{0}\} \times Y^{k+1} : M\mathbf{y}_j = \mathbf{0} \text{ for } 1 \leqslant j \leqslant k+1\}.$$

Since M has null space N_0, we must have $\mathbf{y}_j = \mathbf{0}$ for all j, whence $\mathrm{Ker}(\pi_0)$ is trivial. We may now complete the argument as before, leading to the following conclusion.

LEMMA 3. *Let V_R be the variety (3). Suppose that $\chi(F) = 2$ and that R is odd. Suppose further that we have a point $\mathbf{u} \in F^r$ for which the form*

$$Q = \sum_{i=1}^{r} u_i Q^{(i)} \tag{9}$$

has rank R and null space N and such that $[\mathbf{u}]$ belongs to an irreducible component W of V_R. Then there are at least $1 + \dim(W)$ linearly independent quadratic forms $S^{(i)}$ in the F-pencil (9), all of which vanish on the F-vector space N of codimension R in F^n.

If we now assume the fundamental minimization condition (1), then we may take $n - w = \dim(N)$ so that

$$R = n - \dim(N) = w \geqslant \frac{n}{2r}(1 + \dim(W))$$

and therefore $1 + \dim(W) \leqslant 2rR/n$.

LEMMA 4. *Suppose that (1) holds. Let V_R be the variety (3). Then any point $[\mathbf{u}] \in \mathbb{P}^{r-1}(F)$ for which the form (8) has rank R will belong to an irreducible component W of V_R having $1 + \dim(W) \leqslant 2rR/n$.*

This lemma is the most novel part of our argument. Notice that it tells us nothing about those components W of V_R which do not contain a point defined over F, or for which the only such points are in the subvariety V_{R-1}.

We next estimate how many points can lie in each component W.

LEMMA 5. *Suppose that $V \subseteq \mathbb{A}^r$ is an algebraic set of pure dimension w and degree d. Then*

$$\#V(F) \leqslant dq^w,$$

where $q = \#F$.

This is a relatively standard result, proved along the lines given by Browning and the author [BH05, p. 91]. We use induction on w, the case of $w = 0$ being trivial. Clearly, we can assume that V is absolutely irreducible, by additivity of the degree. When $w \geqslant 1$, there is always at least one index i such that V intersects the hyperplane $u_i = \alpha$ properly for every $\alpha \in \overline{F}$. (If this were not the case, then V must be contained in a hyperplane $u_i = \alpha_i$ for each index i, and so V could contain at most the single point $(\alpha_1, \ldots, \alpha_r)$.) Fixing a suitable index i, we conclude that

$$\#V(F) \leqslant \sum_{\alpha \in F} \#(V \cap \{u_i = \alpha\}).$$

Since $V \cap \{u_i = \alpha\}$ has dimension at most $w - 1$ and degree at most d, we may use the induction hypothesis to conclude that

$$\#(V \cap \{u_i = \alpha\}) \leqslant dq^{w-1},$$

whence the required induction bound follows.

In order to estimate the contribution from all the relevant components W of V_R, we will need information on their degrees as well as their dimensions; for this we use the following result.

Lemma 6. *Let $V \subseteq \mathbb{A}^r$ be an algebraic set defined by the vanishing of polynomials $f_1, \ldots, f_N$ each having total degree at most d. Suppose that V decomposes into irreducible components as $V = \bigcup_{i=1}^{I} V_i$. Then*

$$\sum_{i=1}^{I} \deg(V_i) d^{\dim(V_i)} \leqslant d^r.$$

This is proved by induction on N, with the $N = 1$ case being trivial. We proceed to assume that the result holds for the case N, and prove it for the case $N + 1$. Let us write $H = \{f_{N+1} = 0\}$ for convenience, and suppose that $V_i \cap H$ decomposes into irreducible components as $\bigcup_{j=1}^{J(i)} V_{ij}$. We claim that

$$\sum_{j=1}^{J(i)} \deg(V_{ij}) d^{\dim(V_{ij})} \leqslant \deg(V_i) d^{\dim(V_i)}. \tag{10}$$

Once this is established, we will have

$$\sum_{i=1}^{I} \sum_{j=1}^{J(i)} \deg(V_{ij}) d^{\dim(V_{ij})} \leqslant \sum_{i=1}^{I} \deg(V_i) d^{\dim(V_i)} \leqslant d^r$$

by the induction hypothesis. We will therefore have completed the induction step.

To prove the statement (10), we factor f_{N+1} into absolutely irreducible polynomials $f_{N+1} = g_1 \ldots g_M$, say, and write $H_k = \{g_k = 0\}$. If there is any index k such that $V_i \subseteq H_k$, then $V_i \subseteq H$, whence $V_i \cap H = V_i$ is already irreducible and (10) is trivial. On the other hand, if V_i and H_k intersect properly for every k, then $V_i \cap H_k$ is a union of components V_{ij} for j in some set $S(k) \subseteq \{1, \ldots, J(i)\}$, with $\dim(V_{ij}) = \dim(V_i) - 1$ and

$$\sum_{j \in S(k)} \deg(V_{ij}) \leqslant \deg(V_i) \deg(g_k),$$

by Bézout's theorem. Summing over k then yields

$$\sum_{j=1}^{J(i)} \deg(V_{ij}) \leqslant \deg(V_i) d,$$

and (10) follows in this case, too. This completes the proof of Lemma 6.

We now combine Lemmas 4, 5 and 6 to produce the following result.

LEMMA 7. *Suppose that the quadratic forms $q^{(i)}$ form a minimized system. Then the number $N(R)$ of quadratic forms (8) of rank R, with $\mathbf{u}\in F^r$, satisfies*

$$N(R)\leqslant \left(\frac{q}{R+1}\right)^{[2rR/n]}(R+1)^r$$

whenever $q\geqslant R+1$. Moreover, any non-zero form in the F-pencil has rank at least $2(\lceil n/2r\rceil -1)$.

Suppose that V_R is a union

$$V_R=\bigcup_1^I W_i$$

of irreducible components and that the points $[\mathbf{u}]\in V_R(F)$ lie in components $W_1,\dots,W_L$. Then, applying Lemma 5 to the affine cone over each W_i, we find that

$$N(R)\leqslant \sum_{i=1}^{L}\deg(W_i)q^{1+\dim(W_i)}.$$

However, according to our remarks at the beginning of § 2, and Lemma 1 in particular, the set V_R is defined by equations of degree at most $R+1=d$, say, and hence Lemma 6 yields

$$\sum_{i=1}^{L}\deg(W_i)(R+1)^{1+\dim(W_i)}\leqslant \sum_{i=1}^{I}\deg(W_i)(R+1)^{1+\dim(W_i)}\leqslant (R+1)^r.$$

Lemma 4 shows, however, that $1+\dim(W_i)\leqslant[2rR/n]$ for $i\leqslant L$; so if $q\geqslant R+1$, we will have

$$\begin{aligned}N(R)&\leqslant \sum_{i=1}^{L}\deg(W_i)(R+1)^{1+\dim(W_i)}\left(\frac{q}{R+1}\right)^{1+\dim(W_i)}\\&\leqslant \left(\frac{q}{R+1}\right)^{[2rR/n]}\sum_{i=1}^{L}\deg(W_i)(R+1)^{1+\dim(W_i)}\\&\leqslant \left(\frac{q}{R+1}\right)^{[2rR/n]}(R+1)^r\end{aligned}$$

as required.

For the final observation, we extend the remark made in § 1 in connection with the condition (1). Any form of rank R over F will vanish on a vector space of codimension $(R+1)/2$ if R is odd, or of codimension $(R+2)/2$ if R is even. We may therefore take $w=1+[R/2]$ and deduce that $1+[R/2]\geqslant n/2r$, which gives the required lower bound on R. Note that this argument uses only the minimization condition, and does not require any of Lemmas 2, 3 or 4.

3. Counting zeros

We begin by considering zeros of a system of quadratic forms

$$S^{(i)}(x_1,\dots,x_k)\in F[x_1,\dots,x_k],\quad 1\leqslant i\leqslant I.$$

Consider the set

$$A=\left\{(\mathbf{u},\mathbf{x})\in F^I\times F^k:\sum_{i=1}^{I}u_iS^{(i)}(x_1,\dots,x_k)=0\right\}.$$

We shall count elements of A in two ways. First, we consider how many choices of $\mathbf{u}$ correspond to each $\mathbf{x}$. If $S^{(i)}(\mathbf{x})=0$ for each index i, then there are q^I possible vectors $\mathbf{u}$; otherwise there are q^{I-1} choices. Hence if the system $S^{(i)}(\mathbf{x})=0$ has N zeros in total, we will have

$$\#A = q^I N + q^{I-1}(q^k - N).$$

Alternatively, we can count elements of A according to the value $\mathbf{u}$. In this case we write

$$N(\mathbf{u}) = \#\left\{\mathbf{x}\in F^k : \sum_{i=1}^{I} u_i S^{(i)}(x_1,\ldots,x_k)=0\right\},$$

whence

$$\#A = \sum_{\mathbf{u}} N(\mathbf{u}).$$

We therefore deduce that

$$\begin{aligned} N &= \frac{1}{q^{I-1}(q-1)}\left\{-q^{I+k-1} + \sum_{\mathbf{u}} N(\mathbf{u})\right\} \\ &= \frac{1}{q^{I-1}(q-1)}\left\{\sum_{\mathbf{u}} (N(\mathbf{u}) - q^{k-1})\right\} \\ &= q^{k-I} + \frac{1}{q^{I-1}(q-1)}\left\{\sum_{\mathbf{u}\neq 0} (N(\mathbf{u}) - q^{k-1})\right\}, \end{aligned}$$

since $N(\mathbf{0}) = q^k$.

We proceed to consider the number $N(S)$ of zeros of a single quadratic form $S(x_1,\ldots,x_k)$. If $\mathrm{Rank}(S)=0$, then there are trivially q^k zeros, and if S has rank one there are q^{k-1} zeros. For rank two, there will be $(2q-1)q^{k-2}$ zeros if S factors over F and q^{k-2} zeros otherwise. For larger ranks, there will be at least one non-singular zero by Chevalley's theorem, and a linear change of variables will allow us to write S in the shape

$$S(x_1,\ldots,x_k) = x_1x_2 + S'(x_3,\ldots,x_k).$$

One then finds that there are $2q-1$ possibilities for (x_1,x_2) if $S'=0$ and $(q-1)$ choices otherwise, so that $N(S) = qN(S') + (q-1)q^{k-2}$. An easy induction on k now shows that $N(S)=q^{k-1}$ whenever S has odd rank and that

$$|N(S) - q^{k-1}| = (1-q^{-1})q^{k-R/2}$$

whenever S has even rank R.

We may therefore conclude as follows.

LEMMA 8. *Suppose we have a system of quadratic forms*

$$S^{(i)}(x_1,\ldots,x_k) \in F[x_1,\ldots,x_k], \quad 1 \leqslant i \leqslant I,$$

with N zeros over F. Write N_R for the number of vectors $\mathbf{u}\in F^I$ for which

$$\sum_{i=1}^{I} u_i S^{(i)}(x_1,\ldots,x_k) \tag{11}$$

has rank R, and assume that such a linear combination vanishes only for $\mathbf{u}=\mathbf{0}$. Then

$$|N - q^{k-I}| \leqslant \sum_{1\leqslant t\leqslant k/2} q^{k-I-t} N_{2t}.$$

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

We may now apply Lemma 8 to count non-singular zeros of the system

$$Q^{(1)}(x_1,\dots,x_n),\dots,Q^{(r)}(x_1,\dots,x_n) \tag{12}$$

arising from a minimized system $q^{(1)},\dots,q^{(r)}$. In view of Lemmas 5 and 7, the total number N of common zeros satisfies

$$N \geqslant q^{n-r}\left\{1-\sum_{\lceil n/2r\rceil-1\leqslant t\leqslant n/2} q^{-t}\left(\frac{q}{2t+1}\right)^{[4rt/n]}(2t+1)^r\right\}, \tag{13}$$

providing that $q>n\geqslant 4r+1$. This latter condition is enough to ensure that $q\geqslant 2t+1$ whenever $t\leqslant n/2$. Note that if a non-trivial linear combination (11) were to vanish, we would be able to take $s=1$ and $w=0$ in (1), which is impossible. We remark that the sum in (13) is $O_{r,n}(q^{-1})$ as soon as $n>4r$, and indeed we will have $N\sim q^{n-r}$ as $q\to\infty$ for such n. This is the behaviour we would have if the variety defined by $q^{(1)}=\dots=q^{(r)}=0$ were absolutely irreducible. However, it is not clear whether the minimization condition ensures such irreducibility.

We now have to consider singular zeros for the system (12). Any such zero $\mathbf{x}$ is a singular zero of at least one non-zero form (11) in the pencil, S say. Unless $\mathbf{x}=\mathbf{0}$, we can deduce that S is singular. We proceed to estimate how many zeros the system (12) has which are singular zeros of a given form S of the shape (11). By changing the basis for the pencil, we may indeed assume that $S=Q^{(r)}$. Suppose that S has rank $\rho<n$. Then the singular zeros of S form a vector space of dimension $n-\rho=k$, say, which we may take to be

$$\{(x_1,\dots,x_k,0,\dots,0)\}$$

after a suitable change of variables. It follows that our problem is to count zeros of the new system

$$S^{(1)}(x_1,\dots,x_k),\dots,S^{(r-1)}(x_1,\dots,x_k),$$

where

$$S^{(i)}(x_1,\dots,x_k)=Q^{(i)}(x_1,\dots,x_k,0,\dots,0).$$

According to Lemma 8, there are at most

$$q^{k-(r-1)}\left\{\sum_{0\leqslant t\leqslant k/2} q^{-t}N_{2t}\right\} \tag{14}$$

such zeros, where N_R is the number of linear combinations

$$\sum_{i=1}^{r-1} u_i S^{(i)}(x_1,\dots,x_k) \tag{15}$$

which have rank R.

To estimate N_R, we will use Lemmas 2 and 3 in combination with Lemmas 5 and 6. If $R=2t$ and $W\subseteq\mathbb{P}^{r-2}$ is an irreducible component of the variety of vectors counted by N_R, then Lemmas 2 and 3 show that we have at least $1+\dim(W)$ linearly independent forms from the pencil (15) which vanish simultaneously on a vector space $X\subseteq F^k$ of codimension R. By extending these to forms on F^n, we obtain $1+\dim(W)$ linearly independent forms from the pencil

$$\sum_{i=1}^{r-1} u_i Q^{(i)}(x_1,\dots,x_n)$$

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

which vanish simultaneously on

$$\tilde{X} = \{(x_1, \dots, x_k, 0, \dots, 0) \in F^n : (x_1, \dots, x_k) \in X\}.$$

However, $Q^{(r)}$ also vanishes on $\tilde{X}$, hence the minimization condition (1) yields

$$n - \dim(\tilde{X}) \geqslant \frac{(2 + \dim(W))n}{2r}.$$

Since $\dim(\tilde{X}) = \dim(X) = k - R$, we deduce that

$$\dim(W) \leqslant \frac{2r(n-k+R)}{n} - 2. \tag{16}$$

This allows us to use Lemmas 5 and 6 to conclude that

$$N_R \leqslant \left(\frac{q}{R+1}\right)^{[2r(n-k+R)/n]-1} (R+1)^{r-1}$$

for $q \geqslant R+1$, as in the proof of Lemma 7.

Since $k = n - \rho$, we now find from (14) that the number of zeros of (12) which are singular for a particular S of rank ρ is at most

$$q^{n-\rho-r+1}\left\{\sum_{0\leqslant t\leqslant(n-\rho)/2} q^{-t}\left(\frac{q}{2t+1}\right)^{[2r(\rho+2t)/n]-1}(2t+1)^{r-1}\right\}$$
$$= q^{n-\rho-r}\left\{\sum_{0\leqslant t\leqslant(n-\rho)/2} q^{-t}\left(\frac{q}{2t+1}\right)^{[2r(\rho+2t)/n]}(2t+1)^{r}\right\}.$$

To estimate the total number of singular zeros of (12), we must sum this over all singular forms S and allow for the trivial singular zero $\mathbf{x} = \mathbf{0}$. Although Lemma 7 estimates the number of singular forms of given rank, for our present purposes scalar multiples of a given form S produce the same singular zeros. Hence it suffices to count only one form S from each set of scalar multiples. Thus Lemma 7 shows that the total number of non-trivial singular zeros for the system (12) is at most

$$\frac{q^{n-r}}{q-1}\sum_{\rho=2(\lceil n/2r\rceil-1)}^{n-1}\left(\frac{q}{\rho+1}\right)^{[2r\rho/n]}\frac{(\rho+1)^r}{q^\rho}\sum_{0\leqslant t\leqslant(n-\rho)/2}\left(\frac{q}{2t+1}\right)^{[2r(\rho+2t)/n]}\frac{(2t+1)^r}{q^t}$$

for $q > n$. Note that this latter condition will ensure that $q \geqslant 2t+1$ and that $q \geqslant \rho+1$. After allowing for $\mathbf{x} = \mathbf{0}$, it now follows that the total number of non-singular zeros for the system (12) is at least $q^{n-r}(1 - \sigma_1 - \sigma_2)$ with σ_1 and σ_2 as in the theorem, and the sufficiency of the condition $\sigma_1 + \sigma_2 < 1$ follows.

4. Completion of the proofs

We begin by examining the special case where $n = 4r+1$. With this value of n we have $[4rt/n] = t - 1$ for $2 \leqslant t \leqslant n/2$, whence

$$\sigma_1 = q^{-3r-1} + q^{-1}\sum_{2\leqslant t\leqslant 2r}(2t+1)^{r-t+1}.$$

To evaluate σ_2 we observe that for $n = 4r+1$, the ranges for ρ and t are given by $4 \leqslant \rho \leqslant 4r$ and $0 \leqslant t \leqslant (n-\rho)/2$. Moreover, we have $[2r\rho/n] = (\rho-1)/2$ and $[2r(\rho+2t)/n] = t + (\rho-1)/2$ if ρ

is odd, while $[2r\rho/n] = \rho/2 - 1$ and $[2r(\rho+2t)/n] = t + \rho/2 - 1$ if ρ is even. Thus

$$\sigma_2 = \frac{1}{q-1}\bigg\{q^{-1}\sum_{\nu=2}^{2r-1}\sum_{0\leqslant t\leqslant 2r-\nu}(2\nu+2)^{r-\nu}(2t+1)^{r-t-\nu} + q^{-2}\sum_{\nu=2}^{2r}\sum_{0\leqslant t\leqslant 2r-\nu}(2\nu+1)^{r-\nu+1}(2t+1)^{r-t-\nu+1}\bigg\}.$$

In the case where $r = 3$ we calculate that

$$\sigma_1 = q^{-10} + (32.11\ldots)q^{-1}$$

and

$$\sigma_2 = (14.72\ldots)q^{-1}(q-1)^{-1} + (145.68\ldots)q^{-2}(q-1)^{-1},$$

whence $q \geqslant 37$ is admissible. The other values for $r = 4$ and 8 are calculated similarly.

To prove the general bound it now suffices to assume that $r \geqslant 5$. Note that $(2t+1)^{r-t+1} \leqslant (2r)^{r-1}$ for $2 \leqslant t \leqslant r-1$, while $(2t+1)^{r-t+1} \leqslant 4r+1$ for $r \leqslant t \leqslant 2r$. It follows that

$$\sum_{2\leqslant t\leqslant 2r}(2t+1)^{r-t+1} \leqslant (r-2)(2r)^{r-1} + (r+1)(4r+1) \leqslant (r-1)(2r)^{r-1}.$$

For σ_2 we recall that ν and t are restricted by the conditions $2 \leqslant \nu \leqslant 2r$ and $0 \leqslant t \leqslant 2r-\nu$. We then note that $(2\nu+2)^{r-\nu} \leqslant (2r)^{r-2}$ in each of the cases $2 \leqslant \nu \leqslant r-1$ and $r \leqslant \nu \leqslant 2r-1$, and similarly that $(2t+1)^{r-t-\nu} \leqslant (2r)^{r-2}$ in all cases. Thus

$$\sum_{\nu=2}^{2r-1}\sum_{0\leqslant t\leqslant 2r-\nu}(2\nu+2)^{r-\nu}(2t+1)^{r-t-\nu} \leqslant (2r)^{2r-2}.$$

In the same way, we obtain

$$(2\nu+1)^{r-\nu+1} \leqslant (2r+1)^{r-1} \quad \text{and} \quad (2t+1)^{r-t-\nu+1} \leqslant (2r-1)^{r-1}$$

in all cases, whence

$$\sum_{\nu=2}^{2r}\sum_{0\leqslant t\leqslant 2r-\nu}(2\nu+1)^{r-\nu+1}(2t+1)^{r-t-\nu+1} \leqslant (2r)^{2r}.$$

The condition $\sigma_1 + \sigma_2 < 1$ is therefore satisfied if

$$q^{-r} + (r-1)(2r)^{r-1}q^{-1} + (2r)^{2r-2}q^{-1}(q-1)^{-1} + (2r)^{2r}q^{-2}(q-1)^{-1} < 1.$$

One now readily verifies that the above inequality holds if $r \geqslant 5$ and $q \geqslant (2r)^r$, as required for the theorem.

We turn now to Corollary 2. Since $n \geqslant r^2+1$, we have $\lceil n/2r\rceil - 1 \geqslant (r-1)/2$. Thus if $\phi = 1 - 4/r$, we have

$$\sigma_1 \leqslant q^{-r} + \sum_{t\geqslant (r-1)/2} q^{-\phi t}(2t+1)^r.$$

In the infinite sum the ratio of the terms for $t+1$ and t is

$$q^{-\phi}\left(1+\frac{2}{2t+1}\right)^r \leqslant q^{-\phi}\left(1+\frac{2}{r}\right)^r \leqslant q^{-\phi}e^2.$$

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

Moreover, for a real variable t the function $q^{-\phi t}(2t+1)^r$ is decreasing for $t \geqslant (r-1)/2$, providing only that $q^{\phi} > e^2$. It follows that the first term in the sum is at most $q^{-\phi(r-1)/2}r^r$, whence

$$\sum_{t \geqslant (r-1)/2} q^{-\phi t}(2t+1)^r \leqslant \frac{q^{-\phi(r-1)/2}r^r}{1-q^{-\phi}e^2} \tag{17}$$

and

$$\sigma_1 \leqslant q^{-r} + \frac{q^{-\phi(r-1)/2}r^r}{1-q^{-\phi}e^2}$$

if $r \geqslant 5$ and $q^{\phi} > e^2$.

Similarly, we find that

$$\sigma_2 \leqslant \frac{1}{q-1}\left\{\sum_{\rho=r-1}^{\infty}\sum_{t=0}^{\infty} q^{-\rho\phi - t\phi}(\rho+1)^r(2t+1)^r\right\}.$$

The double sum factors, and the summation over ρ is

$$\sum_{\rho=r-1}^{\infty} q^{-\rho\phi}(\rho+1)^r \leqslant \frac{q^{-\phi(r-1)}r^r}{1-q^{-\phi}e}$$

by an argument closely analogous to that above. For the t-summation we note that the real-variable function $f(\tau) = \tau^r q^{-\phi\tau/2}$ is maximal at $\tau = 2r/(\phi \log q)$, with maximum value $\{2r/(e\phi \log q)\}^r \leqslant (r/e)^r$ if $q^{\phi} > e^2$. Thus

$$\sum_{0 \leqslant t \leqslant (r-2)/2} q^{-\phi t}(2t+1)^r \leqslant \frac{r}{2} q^{\phi/2}(r/e)^r.$$

On combining this with (17) we deduce that

$$\sigma_2 \leqslant \frac{1}{q-1}\left\{\frac{q^{-\phi(r-1)}r^r}{1-q^{-\phi}e}\right\}\left\{\frac{r}{2}q^{\phi/2}(r/e)^r + \frac{q^{-\phi(r-1)/2}r^r}{1-q^{-\phi}e^2}\right\}.$$

Assuming that $q^{\phi} \geqslant 2e^2$, we conclude that

$$\begin{aligned}\sigma_2 &\leqslant q^{-\phi(r-3/2)}r^{2r}\frac{1}{q-1}\left\{\frac{1}{1-1/2e}\right\}\left\{\frac{r}{2}e^{-r} + 2q^{-\phi r/2}\right\}\\ &\leqslant q^{-\phi(r-3/2)}r^{2r}\frac{2}{q}\left\{\frac{r}{2}e^{-r} + 2e^{-r}\right\}\\ &\leqslant q^{-\phi(r-1/2)}r^{2r}C_r,\end{aligned}$$

where

$$C_r = \left\{\frac{r}{2}e^{-r} + 2e^{-r}\right\} \leqslant 1$$

for $r \geqslant 5$.

One may now calculate that $\phi_1 + \phi_2 < 1$ providing that $q^{\phi} \geqslant 4r^2 (\geqslant 2e^2)$. However, the function $(2r)^{1/(r-4)}$ is decreasing for $r \geqslant 5$, so

$$(4r^2)^{1/\phi} = (4r^2)\{(2r)^{1/(r-4)}\}^8 \leqslant 10^8(4r^2)$$

and Corollary 2 follows.

5. Ranks of quadratic forms in characteristic two

In this final section we will prove Lemma 1. Recall that F is any perfect field of characteristic two. Let t_{ij} be indeterminates for $1 \leqslant i \leqslant j \leqslant n$, and write $\mathbf{t} = (t_{11}, t_{12}, \ldots, t_{nn})$. Let

$$Q_{\mathbf{t}}(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} t_{ij} x_i x_j \tag{18}$$

be the corresponding quadratic form, considered as a polynomial in

$$\mathbb{Z}[t_{11}, t_{12}, \ldots, t_{nn}, x_1, \ldots, x_n].$$

We associate a matrix $U(\mathbf{t})$ to $Q_{\mathbf{t}}$, with entries

$$U_{ij} = \begin{cases} t_{ij} & \text{for } i < j, \\ 2t_{ii} & \text{for } i = j, \\ t_{ji} & \text{for } i > j. \end{cases}$$

If $I, J \subseteq \{1, \ldots, n\}$ with $\#I = \#J = R+1$, we define $m^*_{I,J}(\mathbf{t})$ to be the (I, J)-minor of U; this has order $(R+1) \times (R+1)$ and is a form of degree $R+1$ in the variables t_{ij}. If R is even, as we are supposing, then $m^*_{I,I}(\mathbf{t})$ vanishes modulo 2, since it becomes the determinant of a skew-symmetric matrix of odd order when we reduce to $\mathbb{Z}_2$. Thus, if we define

$$m_{I,J}(\mathbf{t}) = \begin{cases} m^*_{I,J}(\mathbf{t}) & \text{for } I \neq J, \\ \frac{1}{2} m^*_{I,I}(\mathbf{t}) & \text{for } I = J, \end{cases}$$

then $m_{I,J}$ will be an integral form in the t_{ij}.

When $I = J$, this is the 'half-determinant' introduced by Kneser in the 1970s; see [Kne02]. A detailed discussion is given by Leep and Schueller [LS02, pp. 395–397], but what we establish here will be sufficient for our purposes. We are grateful to the referee for pointing out these references.

We now map the various $m_{IJ}(\mathbf{t})$ to forms $m_{IJ}(\mathbf{t}; F)$ in $F[t_{11}, \ldots, t_{nn}]$, using the obvious homomorphism from $\mathbb{Z}[t_{11}, \ldots, t_{nn}]$ to $F[t_{11}, \ldots, t_{nn}]$. Let

$$Q(x_1, \ldots, x_n) = \sum_{1 \leqslant i \leqslant j \leqslant n} q_{ij} x_i x_j$$

be a quadratic form over a finite field F of characteristic two. Then we claim that a necessary and sufficient condition for Q to have rank at most R is that the forms $m_{I,J}(\mathbf{t}; F)$ all vanish at $t_{ij} = q_{ij}$. This will clearly suffice for Lemma 1. It will be convenient to call this condition on Q the 'rank condition'.

We now use the fact that any quadratic form over F of rank at least three has a non-singular zero; this is an easy exercise. It follows that any quadratic form over F can be reduced, via a sequence of elementary transformations, to a form of the shape

$$x_1 x_2 + \cdots + x_{2m-2} x_{2m} + q(x_{2m+1}, \ldots, x_n)$$

in which $q(x_{2m+1}, \ldots, x_n)$ either vanishes, or takes one of the forms

$$x_{2m+1}^2 \quad \text{or} \quad x_{2m+1}^2 + x_{2m+1} x_{2m+2} + \mu x_{2m+2}^2.$$

In the third case, $\mu \in F$ is such that q is irreducible over F. The rank of the form will be $2m$, $2m+1$ or $2m+2$, respectively. One can easily verify by explicit calculation that our claim holds if Q is in one of these three canonical shapes.

We proceed to show that if forms Q and Q' with coefficients q_{ij} and q'_{ij}, respectively, are related by an elementary transformation, then Q satisfies the rank condition if and only if Q' does.

https://doi.org/10.1112/S0010437X09004497 Published online by Cambridge University Press

This will be sufficient to complete the proof. Indeed, since elementary transformations are invertible, it will be enough to assume that Q satisfies the rank condition and to deduce that Q' does.

Elementary transformations come in three types. The first kind interchanges two of the variables x_i and x_j, and in this case our result is trivial, since the forms $m_{I,J}(\mathbf{t}; F)$ will merely be permuted. The second type of transformation is $S(\lambda)$, say, which multiplies x_1 by a non-zero scalar λ. If we apply $S(v)$, with an indeterminate v, to the quadratic form (18), then the forms $m^*_{I,J}(\mathbf{t})$ will be multiplied by appropriate powers of v. It follows that $S(\lambda)$ will multiply each $m_{I,J}(\mathbf{q}; F)$ by a power of λ. Hence we again see that if Q satisfies the rank condition, then so does Q'.

The third type of elementary transformation, which we denote by $T(\lambda)$, replaces x_1 by $x_1 + \lambda x_2$. The argument here is similar to that used for $S(\lambda)$. When $T(v)$ is applied to $Q_{\mathbf{t}}$, the forms $m^*_{I,J}(\mathbf{t})$ get replaced by linear combinations of various $m^*_{K,L}(\mathbf{t})$, with coefficients $1, v$ or v^2. Hence, when $T(\lambda)$ is applied to Q, the forms $m_{I,J}(\mathbf{q}; F)$ get replaced by linear combinations of various $m_{K,L}(\mathbf{q}; F)$, with coefficients $1, \lambda$ or λ^2. Again, it is clear that if Q satisfies the rank condition, then so does Q'. This completes the proof of the lemma.

Acknowledgements

Part of this work was carried out at the Hausdorff Institute for Mathematics in Bonn during the Trimestre on Diophantine Equations. The hospitality and financial support of the institute is gratefully acknowledged. The material on quadratic forms in characteristic two owes a great deal to numerous conversations with Damiano Testa, to whom the author is delighted to express his gratitude. This paper has also benefited considerably from the very careful scrutiny of the anonymous referees, who have removed a number of minor errors. Thanks to them are also gratefully recorded.

References

Art65 E. Artin, *The collected papers of Emil Artin* (Addison-Wesley, Reading, MA, 1965).

AK65 J. Ax and S. Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630.

BL65 B. J. Birch and D. J. Lewis, *Systems of three quadratic forms*, Acta Arith. **10** (1964/1965), 423–442.

BH05 T. D. Browning and D. R. Heath-Brown, *Counting rational points on hypersurfaces*, J. Reine Angew. Math. **584** (2005), 83–115.

Dav63 H. Davenport, *Cubic forms in sixteen variables*, Proc. Roy. Soc. Ser. A **272** (1963), 285–303.

Dem56 V. B. Demyanov, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes*, Izv. Akad. Nauk SSSR Ser. Mat. **20** (1956), 307–324.

Has24 H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924), 11–130.

Hea09 D. R. Heath-Brown, *Zeros of p-adic forms*, Proc. London Math. Soc. (3) (2009); doi: 10.1112/plms/pdp043.

Kne02 M. Kneser, *Quadratische formen* (Springer, Berlin, 2002).

Lee84 D. B. Leep, *Systems of quadratic forms*, J. Reine Angew. Math. **350** (1984), 109–116.

LS02 D. B. Leep and L. M. Schueller, *A characterization of nonsingular pairs of quadratic forms*, J. Algebr. Appl. **1** (2002), 391–412.

Mar97 G. Martin, *Solubility of systems of quadratic forms*, Bull. London Math. Soc. **29** (1997), 385–388.

Sch80 S. E. Schuur, *On systems of three quadratic forms*, Acta Arith. **36** (1980), 315–322.

Ter66 G. Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A–B **262** (1966), A612.

D. R. Heath-Brown rhb@maths.ox.ac.uk
Mathematical Institute, 24–29 St. Giles', Oxford, OX1 3LB, UK